

Defense Nuclear Facilities Safety Board



**Software Quality Assurance
at the Department of Energy
Dr. Charles R. Martin**

Background

- Software is used by DOE and its contractors to analyze hazards, to design effective controls, and for automatic control of safety systems.
- As a result, the safety posture of many facilities is strongly dependent on the quality of this underlying body of analysis, design, and control software.

TECH-25

- In January 2000, DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at the Department of Energy Defense Nuclear Facilities*, identified numerous deficiencies in safety-related software at DOE, and the Board asked DOE for a plan of action to address software quality concerns.
- On October 3, 2000, the Board received the DOE corrective action plan (CAP), but found it was not sufficiently responsive to the Board's concerns.

Concerns with DOE's CAP

- On October 23, the Board asked DOE to correct the deficiencies in the CAP:
 - Notice was developed before the analysis of deficiencies was completed and does not clearly set expectations for SQA.
 - Notice does not address SQA within the context of an overall QA program.
 - Key subject matter experts were not involved in preparing the Notice or the CAP.
 - Roles & responsibilities and funding were not adequately addressed.
- The Board has not been provided with a revised plan.

Ongoing Efforts by the Board

- The Board has held two public meetings on QA with SQA as a special interest item.
- The Board's staff has reviewed directives and guidance from other agencies as well as industry consensus standards and visited the NASA Independent Verification and Validation (IV&V) Center.
- The Board's staff has completed a number of on-site reviews of SQA implementation including Y-12, SNL, Hanford, and Pantex.

Observations to Date

- DOE directives and guidance do not clearly set expectations or requirements for SQA, consequently contractor implementing procedures do not have sufficient detail to define a robust process or ensure high quality software products.
- Responsibility and authority for SQA functions within DOE are not adequately defined, nor is there an effective champion for SQA.

Observations to Date (cont.)

- At DOE, there is no consensus set of training requirements for SQA, because there are no clearly defined SQA requirements. Thus there is no formal DOE training program for SQA, and most sites do not have formal SQA training.

Observations to Date (cont.)

- Because software errors can be hard to find, there is a need for a rigorous, well documented process for safety-related software. Adequate consensus standards exist for most SQA processes and products.
- Because software technology continues to evolve, the guidance for SQA also needs to evolve. Interagency working groups are attempting to fill existing gaps and will also address future evolutions with respect to software safety.